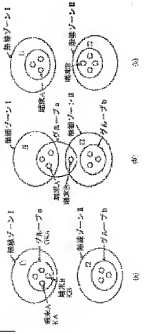
DYNAMIC SECURE GROUP MOBIL OMMUNICATION SYSTEM

Publication number: JP2001203681 (A)
Publication date: 2001-07-27
Inventor(s): ISHII DAISUKE
Applicant(s): ADVANCED MOBILE TELECOMM SECUR
Classification:
- international: ***H04L9/08; H04L12/28; H04M1/725; H04Q7/38;*** **H04L9/08; H04L12/28; H04M1/72; H04Q7/38;** (IPC1-7): H04L9/08; H04L12/28; H04M1/725; H04Q7/38
- European:
Application number: JP20000012651 20000121
Priority number(s): JP20000012651 20000121

Abstract of **JP 2001203681 (A)**

PROBLEM TO BE SOLVED: To provide a dynamic secure group mobile communication system that effectively utilizes a radio frequency so as to enhance the information concealment effect thereby reducing the communication quantity in the group mobile communication using a plurality of radio frequency zones. SOLUTION: When a terminal B in a group (a) shown in Figure 1 (a) moves from a radio zone I to a radio zone II and reaches a state shown in Figure 1 (b), the terminal B informs a base station that the terminal B moves to the radio zone II. The base station changes the group key of the terminal B into a group key of a group (b) in order to assign the terminal B to the group (b) in the radio zone II.; The terminal B reaches a state shown in Figure 1 (c), grouping bridging over the radio zones is eliminated, the frequency can effectively be utilized, the concealing effect of information by the grouping cannot be deteriorated and the communication quantity between the radio zones is not increased.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2001－203681
（P2001－203681A）
(43)公開日　平成13年７月27日(2001.7.27)

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｍ	1/725	５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｌ	9/00　６０１Ｂ	５Ｋ０２７
Ｈ０４Ｌ　12/28		Ｈ０４Ｂ	7/26　１０９Ｒ	５Ｋ０３３
Ｈ０４Ｍ　1/725		Ｈ０４Ｌ	9/00　６０１Ｅ	５Ｋ０６７
			11/00　３１０Ｂ	

審査請求　有　請求項の数4　ＯＬ　（全９頁）

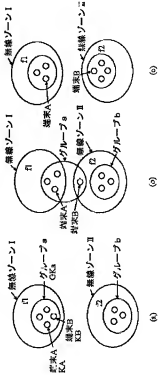
(21)出願番号　特願2000－12851(P2000－12851)
(22)出願日　平成12年１月21日(2000.1.21)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８
(72)発明者　石井　大助
神奈川県横浜市港北区新横浜三丁目20番地８　株式会社高度移動通信セキュリティ技術研究所内
(74)代理人　100099254
弁理士　役　昌明　（外１名）

最終頁に続く

(54)【発明の名称】　ダイナミックセキュアグループ移動通信方式

(57)【要約】
【課題】　複数の無線周波数ゾーンを使用するグループ移動通信において、無線周波数を有効利用し、情報隠蔽効果を上げ、通信量を削減する。
【解決手段】　図１(a)に示すグループａの端末Ｂが、無線ゾーンＩから無線ゾーンIIに移動して、図１(b)に示す状態になると、基地局に無線ゾーンを移動したことを通報する。基地局は、無線ゾーンIIにあるグループｂに端末Ｂを所属させるために、端末Ｂのグループ鍵をグループｂのグループ鍵に変更する。図１(c)に示す状態になり、無線ゾーンをまたぐグループは解消され、周波数を有効利用でき、グループ化による情報の隠蔽効果も低下しないし、無線ゾーン間の通信量も増加しない。



【特許請求の範囲】

【請求項1】　基地局と複数の端末からなり、前記複数の端末を複数の仮想的なグループに分け、それぞれのグループに属する端末に同一のグループ暗号鍵を付し、前記グループ暗号鍵で通信相手あるいは通信内容を暗号化して隠蔽し、複数の無線周波数ゾーンを用いて通信を行なうダイナミックセキュアグループ移動通信方式において、前記基地局に、前記端末の属する無線周波数ゾーンの通報を前記端末から受けて前記端末のグループ暗号鍵を変更する手段と、変更したグループ暗号鍵を前記端末に配送する手段とを設け、前記端末に、個々の端末を識別する端末ＩＤと前記端末それぞれに異なる端末固有の端末暗号鍵とを格納した端末メモリと、前記端末の属する無線周波数ゾーンを検出する手段と、前記端末の属する無線周波数ゾーンを前記基地局に通報する手段とを備えたことを特徴とするダイナミックセキュアグループ移動通信方式。

【請求項2】　１つの無線周波数ゾーンに複数の仮想的なグループを設けたことを特徴とする請求項１記載のダイナミックセキュアグループ移動通信方式。

【請求項3】　前記基地局に、前記端末の属するグループが変更となる端末異動時に端末異動元グループのグループ暗号鍵と端末異動先グループのグループ暗号鍵の少なくとも一方を変更する手段を設けたことを特徴とする請求項１または２記載のダイナミックセキュアグループ移動通信方式。

【請求項4】　前記基地局に、前記端末が前記無線周波数ゾーンを移動したときに前記基地局と該当端末のみしか知らない暗号鍵を使用して新しいグループ暗号鍵を暗号化して配送する手段を設け、前記端末に、前記基地局と該当端末のみしか知らない暗号鍵で情報を暗号化して前記基地局に通知する手段を設けたことを特徴とする請求項１～３のいずれかに記載のダイナミックセキュアグループ移動通信方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ダイナミックセキュアグループ移動通信方式に関し、特に、端末をグループ化してグループ鍵で端末を隠蔽するとともに、端末が無線ゾーンを移動するときにグループを再編成するダイナミックセキュアグループ移動通信方式に関する。

【０００２】

【従来の技術】従来、端末個々の通信を隠蔽する方法として、複数の端末を仮想的なグループによりグループ化し、個々の通信が見えないようにする方法がある。一方、移動通信では、周波数の有効利用を図るために、無線ゾーンが設けられている。無線ゾーン間の電波干渉を防ぐため、隣接する無線ゾーンでは異なった周波数が用いられている。

【０００３】図７(a)に示すように、同一無線ゾーン内に仮想グループが形成された場合には、１つの無線周波数で、仮想グループをカバーできる。図７(b)に示すように、端末が無線ゾーン間を移動した場合、仮想グループの端末をカバーするために、２つの周波数ｆ1，ｆ2が必要となる。通信を行なっている端末を隠蔽する役目をするだけで、実際に通信を行なわない端末にも、無線周波数を割り当てる必要がある。

【０００４】

【発明が解決しようとする課題】しかし、従来のグループ化無線通信システムでは、通信を行なわない端末にも無線周波数を割り当てるので、有限である無線周波数の有効利用とならないという問題があった。また、無線ゾーンから抜けた端末のみを仮想グループから外してしまうと、通信端末の隠蔽効果が小さくなるという問題があった。さらに、無線ゾーン間をまたいで仮想グループを形成すると、無線ゾーン間の通信量が増えてしまうという問題があった。

【０００５】本発明は、上記従来の問題を解決して、無線周波数を有効利用し、隠蔽効果を上げ、通信量を削減することを目的とする。

【０００６】

【課題を解決するための手段】上記の課題を解決するために、本発明では、基地局と複数の端末からなり、複数の端末を複数の仮想的なグループに分け、それぞれのグループに属する端末に同一のグループ暗号鍵を付し、グループ暗号鍵で通信相手あるいは通信内容を暗号化して隠蔽し、複数の無線周波数ゾーンを用いて通信を行なうダイナミックセキュアグループ移動通信方式を、基地局に、端末の属する無線周波数ゾーンを端末から通報を受けてグループ暗号鍵を変更する手段と、変更したグループ暗号鍵を端末に配送する手段とを設け、端末に、個々の端末を識別する端末ＩＤと端末それぞれに異なる端末固有の端末暗号鍵とを格納した端末メモリと、端末の属する無線周波数ゾーンを検出する手段と、無線周波数ゾーンを基地局に通報する手段とを備えた構成とした。

【０００７】このように構成したことにより、無線周波数を有効利用し、隠蔽効果を上げ、通信量を削減することができる。

【０００８】

【発明の実施の形態】以下、本発明の実施の形態について、図１～図６を参照しながら詳細に説明する。

【０００９】（第１の実施の形態）本発明の第１の実施の形態は、無線周波数ゾーンが変わった端末の所属仮想グループを変更するダイナミックセキュアグループ移動通信方式である。

【００１０】図１は、本発明の第１の実施の形態におけるダイナミックセキュアグループ移動通信方式の概念図である。図１において、無線ゾーンＩは、周波数ｆ1で通信する領域である。無線ゾーンIIは、周波数ｆ2で通信する領域である。グループａは、複数の端末を含む仮

想的なグループである。

【0011】図2は、端末装置の機能ブロック図である。図2において、送信部24は、信号を電波に変調して送信する部分である。復号化部27は、受信した暗号文を、端末メモリ22に記録された端末鍵やグループ鍵を用いて復号する部分であり、その結果を信号処理部21に返す。操作部29は、端末に対する指示、通信文、音声などを入力する部分である。表示部30は、操作内容や通信文などを画面や音声によって表示する部分である。端末鍵発生部26は、操作部29などの指示により必要に応じ、端末固有の鍵や乱数を発生、生成する部分である。暗号化部28は、端末メモリ22に記憶された端末鍵やグループ鍵を用いて、操作部29から入力された通信文や鍵に関する情報を暗号化する部分である。この暗号文は、信号処理部21を介し、送信部24から、基地局へ送られる。

【0012】図3は、基地局装置の機能ブロック図である。図3において、暗号化部16は、グループ鍵を端末に配送する場合に、グループ鍵を、基地局メモリ12に記録された端末鍵やグループ鍵で暗号化する部分である。これらの暗号化された暗号文は、信号処理部11を介して送信部14に送られ、電波に変調され、端末に送り出される。通信部19は、複数の基地局間の情報交換を行なう部分である。グループ発生部17は、端末をグループに編成する部分である。グループ鍵発生部18は、グループ発生部17で作られたグループに必要なグループ鍵を生成する部分である。

【0013】図4は、端末装置と基地局装置を組み合わせたシステム構成図である。図5は、端末t3が無線ゾーンIから無線ゾーンIIへ移った後の状態と、端末t3の端末メモリ、管理局メモリの状態を示す図である。図4と図5において、管理局3は、基地局を管理する統括通信局である。

【0014】上記のように構成された本発明の第1の実施の形態におけるダイナミックセキュアグループ移動通信方式の動作を説明する。最初に、通信システムの前提条件を説明する。図1に示すように、無線周波数f1の無線ゾーンIと、無線周波数f2の無線ゾーンIIがある。仮想的に設けられたグループa，b，は、それぞれの無線ゾーンに含まれている。つまり、無線ゾーンIの中にグループaがあり、無線ゾーンIIの中にグループbがある。無線ゾーン間をまたぐグループは存在しない。しかし、移動通信では端末4が常に移動しているので、ひとつの端末が1つの無線ゾーンに常にとどまるということはない。

【0015】図1に示すように、端末Aと端末Bを含む複数の端末で構成されたグループaには、グループ鍵GKaが付与されている。また、各端末には、端末固有の端末鍵が付与されている。端末Aには端末鍵Kaが付与され、端末Bには端末鍵Kbが付与されている。同様に、無線ゾーンII内のグループbに属する各端末にも、それぞれグループ鍵GKbが付与されている。端末鍵もそれぞれ付与されている。

【0016】第2に、基地局装置と端末装置の機能を説明する。図2に示すように、端末装置の受信部23は、基地局からの電波を受けて復号し、信号処理部21に復号された信号を送る。また、受信部23の信号は、ゾーン検出部25に送られ、端末がどの無線ゾーンに位置しているのかというゾーン検出が行われる。このゾーン検出結果も、信号処理部21に送られる。端末メモリ22は、端末鍵、グループ鍵、無線ゾーン、端末IDなどの情報を記憶する部分である。信号処理部21の読出命令によって読み出され、読み出された情報は、信号処理部21に入力される。

【0017】ゾーン検出結果が信号処理部21に入力されると、信号処理部21は、端末メモリ22から、記憶されている無線ゾーンを読み出す。読み出された内容と、ゾーン検出部25から入力された内容とを比較し、異なっていれば、新しい内容を端末メモリ22に書き込む。また、送信部24から基地局に対して、新しい無線ゾーンに加わったことを送信する。

【0018】図3に示す基地局装置の基地局メモリ12は、基地局が管理する端末に関する情報、端末名、端末ID、端末鍵、端末の属するグループ、グループIDなどを記憶している。受信部13は、端末からの電波信号を受信して復調する部分である。復調された信号は、信号処理部11に送られる。暗号文は、復号化部15に送られ、基地局に記憶された端末鍵やグループ鍵などを用いて、適宜復号されて、信号処理部11に入力される。

【0019】第3に、端末の無線ゾーン間の移動について説明する。図1(a)に示すグループaに属する端末のひとつである端末Bが、無線周波数f1の無線ゾーンIから、無線周波数f2の無線ゾーンIIへ移って、図1(b)に示す状態になった時、無線ゾーンIIに存在するグループb(もしくは、新たに編成したグループ)のグループ鍵を端末Bに配送し、端末Bを無線ゾーンIIにあるグループに移動させる。端末Bの端末鍵Kbを使用して、グループ鍵GKbを暗号化して、Kb(GKb)とする。これをグループ鍵GKaで暗号化して、GKa(Kb(GKb))として、無線周波数f1，f2を使用して、全端末に送り出す。

【0020】これを受けたグループaの各端末は、グループ鍵GKaで、GKa(Kb(GKb))を復号して、Kb(GKb)を得る。グループaに属する各端末は、端末鍵でこれを復号しようとする。しかし、端末鍵Kbを持った端末Bのみがグループ鍵GKbを得ることができる。端末Bは、グループ鍵をGKaからGKbに変更し、グループbに所属する。これが、図1(c)に示す状態である。ここでは、端末が無線ゾーンを変わることを移動といい、グループを変わることを異動という。

【0021】以後、グループaに属する端末が通信を行

なう時は、無線周波数ｆ1を使用する。グループｂに属する端末が通信を行なう時は、無線周波数ｆ2を使用する。こうして、グループ化された端末が無線ゾーン間を移動しても、グループが無線ゾーンをまたがることはなく、各グループは1つの無線ゾーン内に存在することになる。

【００２２】第4に、図4と図5を参照して、端末が無線ゾーンを移動する場合のグループ鍵の変更方法を説明する。図4に示すように、端末装置と基地局装置を組み合わせたシステム構成において、無線ゾーンＩを作る基地局1と、無線ゾーンIIを作る基地局2があり、それぞれの無線ゾーンの周波数はｆ1，ｆ2である。基地局1と基地局2に接続され、基地局を管理する管理局3がある。また、基地局1には、無線ゾーンＩに属する端末ｔ1，ｔ2，ｔ3がある。また、基地局2には、無線ゾーンIIに属する端末ｔ4，ｔ5，ｔ6がある。各端末の端末メモリには、端末を識別する端末ＩＤ、端末固有の端末鍵、端末が属するグループを識別するグループＩＤ、グループのグループ鍵、端末の属する無線ゾーンに関する情報が記憶されている。端末ｔ1の端末メモリには、端末ＩＤ、端末鍵、グループＩＤ、グループ鍵、無線ゾーンとして、それぞれＩＤＡ、Ｋｔ1、Ｇａ、ＧＫａ、Ｉが記憶されている。他の端末についても、図4に示す通りである。

【００２３】管理局3は、端末4に関する情報をすべて管理している。端末名に対応して、端末ＩＤ、端末鍵、グループＩＤ、グループ鍵、端末が属するグループ、無線ゾーンとその周波数を記憶している。基地局1と基地局2にも、それぞれ無線ゾーンに属する端末4の情報が基地局メモリに記憶されている。この例では、基地局1の基地局メモリには、端末ｔ1～ｔ3に関する情報が記憶されており、基地局2の基地局メモリには、端末ｔ4～ｔ6に関する情報が記憶されている。

【００２４】このような状態で、端末ｔ3が移動して、無線ゾーンＩから無線ゾーンIIに入る場合を説明する。端末ｔ3は、無線ゾーンIIに入ると、無線ゾーンIIに入ったことを検出する。端末ｔ3は、その端末ＩＤ(ＩＤＢ)をグループ鍵ＧＫａで暗号化し、ＧＫａ(ＩＤＢ)とする。グループＩＤ(Ga)を付し、(Ga，ＧＫａ(ＩＤＢ))として、無線ゾーンIIの周波数ｆ2を使用して基地局2に送る。

【００２５】基地局2は、グループＩＤのGaを見て、グループaのグループ鍵を管理局3に問い合わせる。管理局3からグループ鍵ＧＫａを受け取り、ＧＫａ(ＩＤＢ)を復号する。ＩＤＢにより、端末ｔ3が無線ゾーンIIに入ってきたことを知った基地局2は、管理局3に問い合わせ、端末ｔ3に関する情報を受け取る。基地局2は、これを基地局メモリに記憶する。基地局2に属しているグループのうちのグループｂに、新たな端末ｔ3を所属させる。端末ｔ3の端末鍵Ｋｔ3を使用して、グループｂのグループＩＤ(Gb)とグループ鍵ＧＫｂを暗号化して、Ｋｔ3(Ｇｂ，ＧＫｂ)とする。これをグループ鍵ＧＫａで暗号化して、ＧＫａ(Ｋｔ3(Ｇｂ，ＧＫｂ))とし、グループＩＤ(Ga)を付して、周波数ｆ2で無線ゾーンIIに送信する。

【００２６】グループＩＤがGaの端末ｔ3は、これをグループ鍵ＧＫａで復号して、Ｋｔ3(Ｇｂ，ＧＫｂ)を得る。端末鍵Ｋｔ3でこれを復号して、グループＩＤ(Gb)とそのグループ鍵ＧＫｂを得る。こうして、端末ｔ3は、グループＩＤをGaからGbに変更し、グループ鍵をＧＫａからＧＫｂに変更して、無線ゾーンIIのグループｂに属する。

【００２７】図5は、端末数ｔ3が無線ゾーンＩから無線ゾーンIIへ移った後の状態で、端末ｔ3の端末メモリと管理局メモリの状態を示している。基地局2と端末ｔ3しか知らない端末鍵Ｋｔ3を使用して、端末ｔ3から基地局2に無線ゾーンの連絡を行なえば、基地局2は端末ｔ3を認証できる。また、基地局2からのグループＩＤとグループ鍵を、基地局2と端末ｔ3しか知らない端末鍵Ｋｔ3で暗号化して、基地局2から端末ｔ3へ送れば、端末ｔ3が基地局2を認証することができる。

【００２８】第5に、通話中に無線ゾーンを変更した場合の通信方法を説明する。通話していない端末を、無線ゾーンが変わったときに、移動先の無線ゾーンに属するグループに移しても影響はないが、通話している端末を別グループに移してしまうと、通話ができなくなってしまう。その場合には、通話が完了するまで同一グループにとどめ、通話完了後にグループを変更する。

【００２９】図4に示す状態で、端末ＩＤがＩＤＡである端末ｔ1と、端末ＩＤがＩＤＢである端末ｔ3が通信する場合、共有鍵ＫＡＢを、あらかじめ端末ｔ1と端末ｔ3との間で交換しておく。端末ｔ1は、メッセージMを共有鍵ＫＡＢを使用して、ＫＡ(Ｍ)と暗号化し、端末ＩＤ(ＩＤＢ)を付して、(ＩＤＢ，ＫＡＢ(Ｍ))とする。これをグループ鍵ＧＫａで暗号化して、ＧＫａ(ＩＤＢ，ＫＡＢ(Ｍ))として、グループＩＤ(Ga)を付して基地局1へ送る。

【００３０】基地局1はこれを復号して、ＩＤＢにより端末ｔ3向けのメッセージであることを知る。端末ｔ3は無線ゾーンIIへ移動していることが、基地局1に通知されているので、基地局1は、(Ga，ＧＫａ(ＫＡＢ(Ｍ)))を基地局2へ送る。基地局2は、これを周波数ｆ2の電波で送り出す。端末ｔ3はこれを復号して、メッセージＭを得る。

【００３１】一方、端末ｔ3はメッセージM'を生成し、これを共有鍵ＫＡＢで暗号化し、ＫＡ(Ｍ')とする。グループ鍵ＧＫａで暗号化し、ＧＫａ(ＩＤＡ，ＫＡＢ(Ｍ'))とし、グループＩＤ(Ga)を付して、周波数ｆ2で基地局2へ送る。基地局2は、グループaは自局が管理するグループではないため、グループａを管理する基地局1へ送る。基地局1は、グループ鍵ＧＫａで復号し、

端末ＩＤ(ＩＤＡ)を除いて、再度グループ鍵ＧＫａで暗号化して、ＧＫａ(ＫＡＢ(Ｍ'))とする。グループＩＤ(Ｇａ)を付して、(Ｇａ,ＧＫａ(ＫＡＢ(Ｍ')))として、周波数ｆ1で送り出す。これを受けたグループａの端末は、グループ鍵ＧＫａで復号し、ＫＡＢ(Ｍ')を得る。共有鍵ＫＡＢを有する端末ｔ1のみがこれを復号でき、メッセージＭ'を得る。こうして、通話中に無線ゾーンを移動しても通話が行われる。通話が完了するとグループの変更が行われる。

【００３２】第６に、無線ゾーンが異なる端末間の通信方法を説明する。図４において、異なる無線ゾーンと異なるグループに属する端末ｔ1と端末ｔ6が通信を行なう場合、端末ｔ1はメッセージＭを生成し、あらかじめ端末ｔ6と共有した共有鍵Ｋ16を使用して、メッセージＭを暗号化して、Ｋ16(Ｍ)とする。これに、送信先端末ｔ6の端末ＩＤ(ＩＤt6)を付し、(ＩＤt6,Ｋ16(Ｍ))とする。グループ鍵ＧＫａで暗号化して、ＧＫａ(ＩＤt6,Ｋ16(Ｍ))とする。グループＩＤのＧａを付し、(Ｇａ,ＧＫａ(ＩＤt6,Ｋ16(Ｍ))として、周波数ｆ1で基地局１に送り出す。

【００３３】基地局１はこれを受け、グループ鍵ＧＫａで復号して、(ＩＤt6,Ｋ16(Ｍ))から、端末ｔ6へのメッセージであることを知る。端末ｔ6が、基地局１に所属していないため、管理局３へ問い合わせを行なう。基地局２に所属していることを確認し、(ＩＤt6,Ｋ16(Ｍ))を、基地局２へ送る。基地局２は、端末ｔ6の属するグループｂのグループ鍵ＧＫbで、Ｋ16(Ｍ)を暗号化し、(Ｇb,ＧＫb(Ｋ16(Ｍ)))を、周波数ｆ2で送り出す。

【００３４】無線ゾーンIIにあるグループｂの端末は、グループ鍵ＧＫbでこれを復号して、Ｋ16(Ｍ)を得る。共有鍵Ｋ16を保持する端末ｔ6のみが、これを共有鍵で復号して、メッセージＭを得ることができる。端末ｔ6から端末ｔ1への送信は、端末ｔ1から端末ｔ6への逆の処理が行われて、端末ｔ6のメッセージが端末ｔ1に送られる。このようにして、端末ｔ1と端末ｔ6間で送受信が相互に行われて通信ができる。

【００３５】上記のように、本発明の第１の実施の形態では、ダイナミックセキュアグループ移動通信方式を、無線周波数ゾーンが変わった端末の仮想グループを、移動先の無線ゾーン内のグループに変更する構成としたので、無線ゾーンをまたぐグループを無くして、周波数を有効利用できる。

【００３６】(第２の実施の形態) 本発明の第２の実施の形態は、グループ構成が変わったグループのグループ鍵を変更するダイナミックセキュアグループ移動通信方式である。

【００３７】図６は、本発明の第２の実施の形態におけるダイナミックセキュアグループ移動通信方式の全体構成図である。第２の実施の形態におけるダイナミックセキュアグループ移動通信方式の基本的な構成は、第１の実施の形態と同じである。

【００３８】端末の異動に関係したグループのグループ鍵を変更する方法を説明する。端末が異動して抜けたグループ、あるいは端末が新たに加わるグループは、すべてのグループ鍵を変更してしまうことが、セキュリティを厳重にするために有効である。図４において、基地局２は、端末ｔ3が加わるグループｂのグループＩＤをＧｂ'と変更し、そのグループ鍵をＧＫb'と変更する。これらをグループ鍵ＧＫbで暗号化し、ＧＫb(Ｇb',ＧＫb')とする。一方、加わる端末ｔ3には予め、ＧＫａ(Ｋt3(ＧＢ',ＧＫb'))とする。それぞれのグループＩＤを付して送信する。

【００３９】グループｂに属していた端末t4, t5, t6は、ＧＫb(Ｇb',ＧＫb')をグループ鍵ＧＫbで復号して、(Ｇb',ＧＫb')を得て、グループＩＤをＧb'とし、グループ鍵をＧＫb'とする。また、移動してグループｂに入った端末ｔ3は、グループ鍵ＧＫbと端末鍵Ｋt3で復号して、(Ｇb',ＧＫb')を得て、新しいグループＩＤ(Ｇb')とグループ鍵ＧＫb'に変更する。

【００４０】また、端末ｔ3が抜けたグループａに残った端末ｔ1, ｔ2に対しては、基地局１は、グループＩＤをＧａ'とし、グループ鍵をＧＫａ'とする。(Ｋt1(Ｇａ',ＧＫａ'),Ｋt2(Ｇａ',ＧＫａ'))を生成し、これをグループ鍵ＧＫaで暗号化して、ＧＫａ(Ｋt1(Ｇａ',ＧＫａ'),Ｋt2(Ｇａ',ＧＫａ'))とし、グループＩＤ(Ｇａ)を付して各端末に配送する。

【００４１】グループａに属する端末ｔ1, ｔ2は、グループ鍵ＧＫａを使ってこれを復号し、(Ｋt1(Ｇａ',ＧＫａ'),Ｋt2(Ｇａ',ＧＫａ'))を得る。それぞれの端末鍵Ｋt1, Ｋt2を使って復号し、(Ｇａ',ＧＫａ')を得て、これを新たなグループＩＤ、グループ鍵として使用する。この時、端末ｔ3がグループ鍵ＧＫａを保持していて、ＧＫａ(Ｋt1(Ｇａ',ＧＫａ'),Ｋt2(Ｇａ',ＧＫａ'))を復号できても、端末ｔ3の端末鍵Ｋt3で暗号化された情報がないため、(Ｇａ',ＧＫａ')を得ることはできない。

【００４２】このようにして、端末の抜けや加入などによりグループ構成に変化があった場合、グループ鍵を変えて、図６に示す状態にすることができる。当然、どちらか一方のグループ鍵のみを変えることもできる。

【００４３】上記のように、本発明の第２の実施の形態では、ダイナミックセキュアグループ移動通信方式を、グループ構成が変わったグループのグループ鍵を変更する構成としたので、セキュリティを高めることができる。

【００４４】

【発明の効果】以上の説明から明らかなように、本発明では、基地局と複数の端末からなり、複数の端末を複数の仮想的なグループに分け、それぞれのグループに属する端末に同一のグループ暗号鍵を付し、グループ暗号鍵で通信相手あるいは通信内容を暗号化して隠蔽し、複数

の無線周波数ゾーンを用いて通信を行なうダイナミックセキュアグループ移動通信方式を、基地局に、端末の属する無線周波数ゾーンを端末から通報を受けてグループ暗号鍵を変更する手段と、変更したグループ暗号鍵を端末に配送する手段とを設け、端末に、個々の端末を識別する端末ＩＤと端末それぞれに異なる端末固有の端末暗号鍵とを格納した端末メモリと、端末の属する無線周波数ゾーンを検出する手段と、無線周波数ゾーンを基地局に通報する手段とを備えた構成としたので、異なった無線周波数ゾーンにまたがったグループを構成する必要がなくなって電波の有効利用ができ、移動した端末を隠蔽する効果を維持することができ、無線ゾーン間に存在するグループを無くして基地局の通信量を少なくすることができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態におけるダイナミックセキュアグループ移動通信方式の概念図、

【図２】本発明の第１の実施の形態におけるダイナミックセキュアグループ移動通信方式の端末装置の機能ブロック図、

【図３】本発明の第１の実施の形態におけるダイナミックセキュアグループ移動通信方式の基地局装置の機能ブロック図、

【図４】本発明の第１の実施の形態におけるダイナミックセキュアグループ移動通信方式の全体構成図、

【図５】本発明の第１の実施の形態におけるダイナミックセキュアグループ移動通信方式の端末異動後の全体構成図、

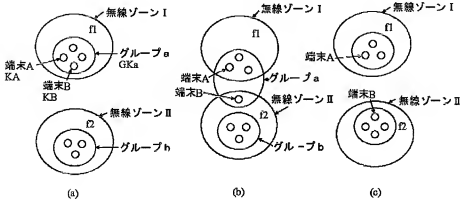
【図６】本発明の第２の実施の形態におけるダイナミックセキュアグループ移動通信方式の全体構成図、

【図７】従来のグループ移動通信方式の概念図である。

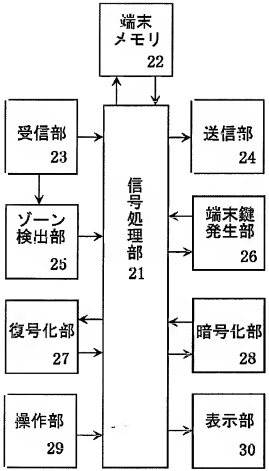
【符号の説明】

1 基地局
2 基地局
3 管理局
4 端末
11 信号処理部
12 基地局メモリ
13 受信部
14 送信部
15 復号化部
16 暗号化部
17 グループ発生部
18 グループ鍵発生部
19 通信部
21 信号処理部
22 端末メモリ
23 受信部
24 送信部
25 ゾーン検出部
26 端末鍵発生部
27 復号化部
28 暗号化部
29 操作部
30 表示部

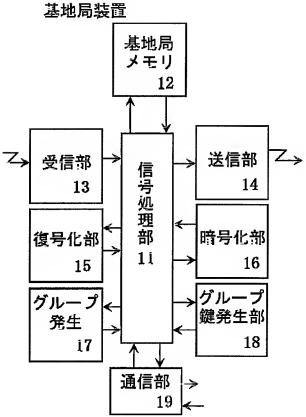
【図１】



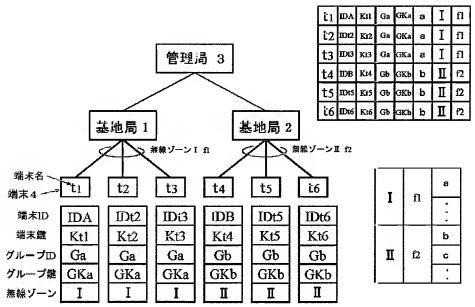
【図2】


端末
メモリ
22
受信部
23
信号処理部
21
送信部
24
ゾーン
検出部
25
端末鍵
発生部
26
復号化部
27
暗号化部
28
操作部
29
表示部
30

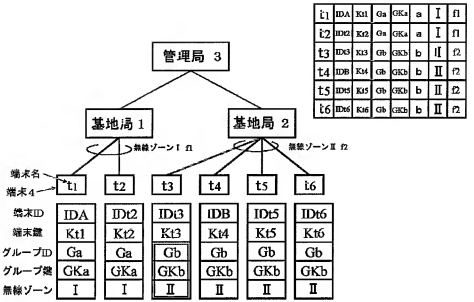
【図3】


基地局装置
基地局
メモリ
12
受信部
13
信号処理部
11
送信部
14
復号化部
15
暗号化部
16
グループ
発生
17
グループ
鍵発生部
18
通信部
19

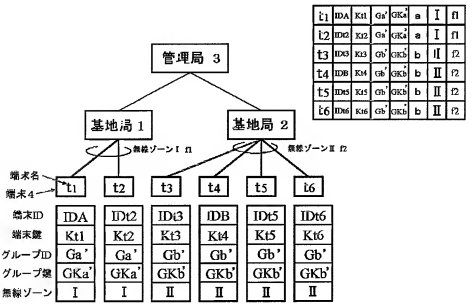
【図4】


管理局 3
基地局 1
基地局 2
無線ゾーンⅠ f1
無線ゾーンⅡ f2
端末名
端末 4
t1
t2
t3
t4
t5
t6
端末ID
IDA
IDt2
IDt3
IDB
IDt5
IDt6
端末鍵
Kt1
Kt2
Kt3
Kt4
Kt5
Kt6
グループID
Ga
Ga
Ga
Gb
Gb
Gb
グループ鍵
GKa
GKa
GKa
GKb
GKb
GKb
無線ゾーン
Ⅰ
Ⅰ
Ⅰ
Ⅱ
Ⅱ
Ⅱ
Ⅰ f1 a
b
Ⅱ f2 c

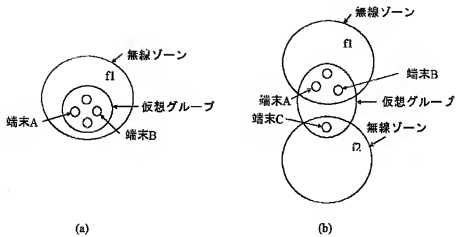
【図5】


t1 IDA Kt1 Ga GKa a I f1
t2 IDt2 Kt2 Ga GKa a I f1
t3 IDt3 Kt3 Gb GKb b II f2
t4 IDB Kt4 Gb GKb b II f2
t5 IDt5 Kt5 Gb GKb b II f2
t6 IDt6 Kt6 Gb GKb b II f2
管理局 3
基地局 1
基地局 2
無線ゾーンI f1
無線ゾーンII f2
端末名
端末4
t1
t2
t3
t4
t5
t6
端末ID
IDA
IDt2
IDt3
IDB
IDt5
IDt6
端末鍵
Kt1
Kt2
Kt3
Kt4
Kt5
Kt6
グループID
Ga
Ga
Gb
Gb
Gb
Gb
グループ鍵
GKa
GKa
GKb
GKb
GKb
GKb
無線ゾーン
I
I
II
II
II
II

【図6】


t1 IDA Kt1 Ga' GKa' a I f1
t2 IDt2 Kt2 Ga' GKa' a I f1
t3 IDt3 Kt3 Gb' GKb' b II f2
t4 IDB Kt4 Gb' GKb' b II f2
t5 IDt5 Kt5 Gb' GKb' b II f2
t6 IDt6 Kt6 Gb' GKb' b II f2
管理局 3
基地局 1
基地局 2
無線ゾーンI f1
無線ゾーンII f2
端末名
端末4
t1
t2
t3
t4
t5
t6
端末ID
IDA
IDt2
IDt3
IDB
IDt5
IDt6
端末鍵
Kt1
Kt2
Kt3
Kt4
Kt5
Kt6
グループID
Ga'
Ga'
Gb'
Gb'
Gb'
Gb'
グループ鍵
GKa'
GKa'
GKb'
GKb'
GKb'
GKb'
無線ゾーン
I
I
II
II
II
II

【図7】



フロントページの続き

Fターム(参考) 5J104 AA01 AA16 EA01 EA04 EA18
JA03 MA05 NA02 PA01
5K027 AA11 CC08
5K033 AA08 DA01 DA19
5K067 AA30 CC13 DD17 EE02 EE10
HH21 HH23 HH36